IN THE SPECIFICATION:

Please replace the last paragraph starting on page 5, line 30, and continuing onto page 6 with the following new paragraph:

-- How to delegate the right to decrypt from one key holder to another in secure and efficient ways is the subject of proxy encryption. Very recently, some specific proxy encryption schemes have been proposed to convert messages encrypted for one key into messages encrypted for another without revealing secret decryption keys and original messages to the public. Mambo and Okamoto have described three proxy encryption schemes for the ElGamal and RSA encryption schemes. M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts," *IEICE Trans. on Fundamentals*, Vol. E80-A, No. 1, pp. 54-63 (1997). For the situation mentioned above, their schemes have better computational performance over the re-encryption scheme, but for security reasons require the presence of the original key holder Alice in the message conversion. Moreover, the schemes themselves do not help specify who is the key holder that Alice wants to delegate the decryption right to. The scheme proposed by Blaze and Strauss, on the other hand, does not have these shortcomings. It is a modification of the ElGamal encryption scheme. M. Blaze and M. Strauss, "Proxy Cryptography," Draft, AT&T Research Labs, ftp://ftp.research.att.com/distlmab/proxy.ps (May 1997). One very appealing feature of the Blaze and Strauss scheme is that it permits communicating proxy related information and performing the message conversion in public. But it introduces a more serious problem: it is commutative in the sense that Bob is able to obtain Alice's decryption key. This type of commutativity makes the proxy encryption scheme obsolete, as the entire scheme can be well simplified to giving Alice's key to Bob and letting Bob decrypt. Another issue (not necessarily a problem) created by this scheme is that once Bob has been granted the decryption right by Alice, he can decrypt all messages that are originally for Alice. This message independence may be useful in some cases, such as self-delegation, but it is not desirable in many practical applications, such as where the original key holder wants to be selective in choosing which messages are allowed to utilize the delegated decryption.--

Please replace the last paragraph starting on page 6, line 28, and continuing onto page 7 with the following new paragraph:

A2

-- In this disclosure, two new proxy encryption schemes are then introduced. They are all based on the ElGamal public-key encryption scheme and have comparable computational performance. Essentially, they have retained the following desirable features of the existing schemes: (i) public: the presence of the original key holder is not required after proxy information is generated, and proxy related information and operations can be communicated and conducted in public; (ii) non-commutative: key holders do not have to trust each other in regard to their private decryption keys; and (iii) restricted: the key holder to whom the decryption right is delegated to is specified, and the proxy information (key) is message dependent. --

Please replace the first full paragraph on page 9 with the following new paragraph:

-- The distributor 114 then passes modified content 116 to a user 118. In a typical electronic distribution model, the modified content 116 represents a re-encrypted version of the original encrypted content 112; the distributor 114 first decrypts the original content 112 and then re-encrypts it with the user 118's public key; that modified content 116 is customized solely for the single user 118. The user 118 is then able to use his private key to decrypt the modified content 116 and view the original content 112. --

Please replace the first full paragraph on page 20 with the following new paragraph:

-- As indicated in the introduction, the goal of proxy encryption is to delegate the decryption right from one to another in secure and efficient ways. For the discussion that follows, it is convenient to define the roles of parties that may be involved in proxy encryption. The two most important roles are those of grantor and grantee. A *grantor* is an original key holder of encrypted messages who wants to delegate the decryption right to someone else. A *grantee* is a key holder designated to perform decryption on behalf of a grantor and thus act as grantor's decryption proxy. In the motivating example in the introduction, Alice is the grantor while Bob is the grantee. Other roles may include an *encryptor* who is the one that originally encrypts messages for the grantor, and a *facilitator* who may help to perform some message processing tasks, such as transforming messages encrypted for the grantor into messages encrypted for the grantee. Certainly, it is not necessary that all these roles are played by different parties. For example, a party may play roles of the grantor and facilitator, as in the Mambo and Okamoto schemes discussed below.

--

Please replace the first full paragraph on page 23 with the following new paragraph:

A5

-- Proxy encryption schemes may vary according to their application requirements. They can be categorized according to many aspects. Obvious ones include whether they are public-key or private-key based, and whether their security measures are perfect in the information theoretical sense or rely on intractability of some computational problems. The following aspects are related to the proxy key and transformation. --

Please replace the second full paragraph on page 43 with the following new paragraph:

-- While the various aspects of the present invention have been described with reference to several aspects and their embodiments, those embodiments are offered by way of example, not by way of limitation. The foregoing detailed description of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously many modifications and variations are possible in light of the above teaching. The described embodiments were chosen in order to best explain the principles of the invention and its practical applications to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. Those skilled in the art will be enabled by this disclosure to make various obvious additions or modifications to the embodiments described herein; those additions and modifications are deemed to lie within the scope of the present invention. It is intended that the scope of the invention be defined by the claims appended hereto. --